Math 332 Winter 2023, Lecture 16: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.14. An introduction to divisibility theory

Elementary number theory is the study of integers and their various features and properties. Divisibility is among the most important of these features, and various notions downstream of it (prime numbers, congruences, etc.) form the stem of classical number theory.

Divisibility theory is about generalizing these notions and properties from integers to elements of other commutative rings. Some things generalize easily, some less so, and some don't generalize at all. Often, properties only hold if the ring satisfies certain conditions. In this section, we will explore some basics of divisibility theory without going anywhere deep. See §2.14 and §2.15 in the text for a slightly deeper treatment (and for more details). Even more can be found in textbooks such as [Knapp16] or [DumFoo04, Chapter 8].

1.14.1. Principal ideal domains

In Lecture 15, we defined **Euclidean rings** to be commutative rings that have a "division with remainder" procedure. The quotient and the remainder need not be unique, but the remainder must be in some way smaller than the "number" (= ring element) that we are dividing by. ("Smaller" means "smaller norm".)

We also defined **Euclidean domains** to be integral domains that are Euclidean rings. (Recall: An integral domain is a nontrivial commutative ring that has no zero-divisors.)

Proposition 1.13.3 says the following:

Proposition 1.14.1. In a Euclidean ring, every ideal is principal.

This motivates the following concept:

Definition 1.14.2. An integral domain R is said to be a **principal ideal domain** (for short, **PID**) if each ideal of R is principal.

Thus, Proposition 1.14.1 yields the following:

Proposition 1.14.3. Any Euclidean domain is a PID.

The converse is not true, but counterexamples are rather exotic. One such counterexample is the ring

$$\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}, \qquad \text{where } \alpha = \frac{1+\sqrt{-19}}{2}.$$

This ring is a PID, but not Euclidean. (This is proved in [DumFoo04, end of §8.1]. See a textbook on algebraic number theory, specifically on quadratic number fields – such as [Lehman19] – for much more about these kinds of rings.)

1.14.2. Divisibility in commutative rings

Let us next generalize (or almost-generalize) some classical concepts of number theory to commutative rings:

> **Definition 1.14.4.** Let R be a commutative ring.
>
> Let $a \in R$.
>
> **(a)** A **multiple** of a means an element of the form ac with $c \in R$. In other words, it means an element of the principal ideal aR.
>
> **(b)** A **divisor** of a means an element $d \in R$ such that a is a multiple of d. We write "$d \mid a$" for "d is a divisor of a".
>
> Now, let $a \in R$ and $b \in R$.
>
> **(c)** A **common divisor** of a and b means an element of R that is a divisor of a and a divisor of b at the same time.
>
> **(d)** A **common multiple** of a and b means an element of R that is a multiple of a and a multiple of b at the same time.
>
> **(e)** A **greatest common divisor** (short: **gcd**) of a and b means a common divisor d of a and b such that **every** common divisor of a and b is a divisor of d.
>
> **(f)** A **lowest common multiple** (short: **lcm**) of a and b means a common multiple m of a and b such that **every** common multiple of a and b is a multiple of m.

The notions of "multiple" and "divisor" we just introduced are straightforward generalizations of the eponymous classical notions from elementary number theory. But our new notions of "gcd" and "lcm" are defined somewhat differently: In contrast to elementary number theory, we cannot take the words "greatest" and "lowest" literally (since there is no ordering defined on the elements of R in general), and thus we had to resort to characterizing gcds and lcms in terms of divisibility alone (as opposed to maximality or minimality). As a consequence:

- It is not guaranteed that a gcd and an lcm of a and b in a given commutative ring R exist in the first place. And indeed, we will see some examples where they don't.

- Our new definitions of gcds and lcms are slightly more lax than the classical ones. In fact, in classical elementary number theory, the gcd of 4 and 6 is 2. However, according to our new definition (Definition 1.14.4 **(e)**), a gcd of 4 and 6 is 2, but another gcd of 4 and 6 is -2. As far as divisibility is concerned, the sign of an integer is irrelevant (if $a \mid b$, then $-a \mid b$ and $a \mid -b$), so a gcd and an lcm (as we just defined them) are unique only up to sign. This is why we say "a gcd" rather than "the gcd" in Definition 1.14.4 (and likewise for lcms). Nevertheless, gcds and lcms are usually unique in a certain sense (think of it as "unique up to sign", but again slightly generalized). We will see this soon.

1.14.3. Gcds and lcms

Let us pin down how the above general notions of gcd and lcm relate to the corresponding notions in elementary number theory:

Proposition 1.14.5. Let a and b be two integers. Let $g = \gcd(a, b)$ and $\ell = \operatorname{lcm}(a, b)$ in the sense of elementary number theory. Then:

(a) The gcds of a and b in our new sense (i.e., in the sense of Definition 1.14.4 **(e)**) are g and $-g$.

(b) The lcms of a and b in our new sense (i.e., in the sense of Definition 1.14.4 **(f)**) are ℓ and $-\ell$.

Proof. Easy if you remember your number theory. (For details, see Proposition 2.14.5 in the text.) □

Let us look at arbitrary commutative rings R now. In this generality, two elements might not even have a gcd. For example, if R is the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \ \mid \ a, b \in \mathbb{Z}\right\},$$

then the elements $a = 4$ and $b = 2\left(1 + \sqrt{-3}\right)$ have neither a gcd nor an lcm. So the existence of gcds and lcms is not god-given. What about uniqueness?

1.14.4. Associate elements

We need to generalize "uniqueness up to sign" for integers. The appropriate generalization is the following:

Definition 1.14.6. Let R be a commutative ring. Let $a, b \in R$. We say that a is **associate** to b (and we write $a \sim b$) if there exists a unit u of R such that $a = bu$.

The relation "associate" is easily seen to be symmetric (because if u is a unit, then u^{-1} is a unit), so we can just as well say "a and b are associate" for $a \sim b$.

Here are a few examples:

- Two integers a and b are associate in $\mathbb{Z}$ if and only if $a = \pm b$.
- Two nonzero elements a and b of a field are always associate, since $a = b \cdot \dfrac{a}{b}$. The element 0 is associate only to itself.
- Let F be a field. In the polynomial ring $F[x]$, any nonzero polynomial $f \in F[x]$ is associate to a monic polynomial (since its leading coefficient is a unit, and dividing f by this coefficient results in a monic polynomial).
- It is not hard to show[1] that the only units of the ring $\mathbb{Z}[i]$ are the four Gaussian integers 1, i, -1, $-i$. So two Gaussian integers α and β are associate if and only if α is one of β, $i\beta$, $-\beta$ and $-i\beta$. (This can be nicely visualized on the Argand diagram: The points corresponding to β, $i\beta$, $-\beta$ and $-i\beta$ are the images of β under rotations around the origin by 0°, 90°, 180° and 270°.)

Here are some general properties of associateness:

Proposition 1.14.7. Let R be a commutative ring. The relation $\sim$ is an equivalence relation.

Proposition 1.14.8. Let R be an integral domain. Let $a, b \in R$ be such that $a \mid b$ and $b \mid a$. Then, $a \sim b$.

For the proofs (which are fairly easy), see the text (§2.14.4).

Proposition 1.14.8 becomes false if we drop the "integral domain" part. However, the counterexamples are rather sophisticated.

Associate elements "look the same" to divisibility, by which I mean that a divisibility relation of the form $a \mid b$ remains equivalent if we replace a by an element associate to a or replace b by an element associate to b. In other words:

Proposition 1.14.9. Let R be a commutative ring. Let $a, b, a', b' \in R$ be such that $a \sim a'$ and $b \sim b'$. Then, $a \mid b$ if and only if $a' \mid b'$.

1.14.5. Uniqueness of gcds and lcms in an integral domain

We can now state the uniqueness of gcds and lcms in the form in which it does hold:

Proposition 1.14.10. Let R be an integral domain. Let $a, b \in R$. Then:

(a) Any two gcds of a and b are associate (i.e., associate to each other).

(b) Any two lcms of a and b are associate (i.e., associate to each other).

[1] See Corollary 1.15.7 in Lecture 17.

Proof. **(a)** Let g and h be two gcds of a and b. We must prove that $g \sim h$.

Since h is a gcd of a and b, we know that h is a common divisor of a and b.

Since g is a gcd of a and b, we know that every common divisor of a and b is a divisor of g. Since h is a common divisor of a and b, we thus conclude that $h \mid g$.

Similarly, $g \mid h$. Thus, $g \mid h$ and $h \mid g$, so that Proposition 1.14.8 yields $g \sim h$. This proves part **(a)**. (Note that this argument is a common trope in algebra.)

(b) Analogous to part **(a)**. □

So much for the uniqueness of gcds and lcms. Their existence is a subtler question.

1.14.6. Existence of gcds and lcms in a PID

At least in PIDs (and thus in Euclidean domains), gcds and lcms always exist:

Theorem 1.14.11. Let R be a PID (for example, a Euclidean domain). Let $a, b \in R$. Then, there exist a gcd and an lcm of a and b.

Somewhat more concretely:

Proposition 1.14.12. Let R be a commutative ring. Let $a, b, c \in R$. Then:

(a) If $aR + bR = cR$, then c is a gcd of a and b.

(b) If $aR \cap bR = cR$, then c is an lcm of a and b.

Note that the aR, bR and cR here are principal ideals of R. Thus, the equality $aR + bR = cR$ is an equality of ideals, not of elements. In particular, it has nothing to do with the equality $a + b = c$. Translated into the language of elements, the equality $aR + bR = cR$ is saying "every sum of a multiple of a with a multiple of b is a multiple of c, and conversely".

Proof of Proposition 1.14.12. **(a)** Assume that $aR + bR = cR$. Thus, $c = c \cdot 1 \in cR = aR + bR$, so that we can write c as $c = ax + by$ for some $x, y \in R$. Consider these x, y. Also, $a = a \cdot 0 + b \cdot 1 \in aR + bR = cR$, so that a is a multiple of c. Similarly, b is a multiple of c. These two sentences show that c is a common divisor of a and b.

Moreover, any common divisor d of a and b satisfies $d \mid a \mid ax$ and $d \mid b \mid by$ and therefore $d \mid ax + by = c$. In other words, any common divisor d of a and b is a divisor of c. Since c is a common divisor of a and b, we thus conclude that c is a gcd of a and b. This proves Proposition 1.14.12 **(a)**.

(b) The condition $aR \cap bR = cR$ is just saying that the multiples of a that happen to be multiples of b at the same time are precisely the multiples of c. If you think about this, this is saying precisely that c is an lcm of a and b. Thus, Proposition 1.14.12 **(b)** follows. □

Note that the converse of Proposition 1.14.12 **(a)** is false (two elements a and b can have a gcd even if the ideal $aR + bR$ is not principal!), whereas the converse of Proposition 1.14.12 **(b)** is true (for the same reason as Proposition 1.14.12 **(b)** itself).

Proof of Theorem 1.14.11. The ideal $aR + bR$ is principal (since R is a PID, so that every ideal of R is principal), and thus can be written as cR for some $c \in R$. This c must then be a gcd of a and b (by Proposition 1.14.12 **(a)**). Thus, a and b have a gcd. Similarly, a and b have an lcm. This proves Theorem 1.14.11. □

Theorem 1.14.11 gives no actual algorithm for finding gcds and lcms. However, if R is a Euclidean ring, then such an algorithm for gcds can be given, and in fact is a straightforward generalization of the classical Euclidean algorithm. An lcm can then be obtained by the formula

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) \sim ab,$$

which holds for any two elements a, b of an integral domain R that have a gcd and an lcm. The proof of this formula can be found in Winter 2021 homework set #2 Exercise 3.

Last time, we saw a bunch of Euclidean domains (the most important one being $\mathbb{Z}[i]$, the Gaussian integers). Thus, in each of these domains, there are well-defined concepts of gcds and lcms, which satisfy the same rules as for integers except for not being unique on-the-nose (but only unique up to associateness).

1.14.7. Irreducible and prime elements

Next, let us generalize prime numbers from the ring $\mathbb{Z}$ to an arbitrary commutative ring R. There are two ways to do so, and both are useful. In fact, recall that prime numbers in $\mathbb{Z}$ can be characterized in two ways:

1. They are the integers $p > 1$ that have no positive divisors besides 1 and p. In other words, they are the integers $p > 1$ such that whenever two integers $a, b \in \mathbb{Z}$ satisfy $ab = p$, at least one of a and b is ± 1.

2. They are the integers $p > 1$ with the property that if $p \mid ab$ (for two integers a and b), then $p \mid a$ or $p \mid b$.

These two characterizations are equivalent, as you should know from high school(?). However, if we try to generalize them to arbitrary commutative rings, their equivalence breaks down. Both characterizations are important, so they both have standard names. Characterization 1 defines "**irreducible** elements", and characterization 2 defines "**prime** elements". More precisely, we define these concepts as follows:

Definition 1.14.13. Let R be a commutative ring. Let $r \in R$ be nonzero and not a unit.

(a) We say that r is **irreducible** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $ab = r$, at least one of a and b is a unit.

(b) We say that r is **prime** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $r \mid ab$, we have $r \mid a$ or $r \mid b$.

Note that we have replaced the condition "$p > 1$" in both characterizations of prime numbers by "r is nonzero and not a unit" in the general setting, in order for it to make sense in an arbitrary ring. As a consequence, our notions of "irreducible" and "prime" are somewhat laxer than the classical concept of a prime number, since they allow negative integers in the case of $R = \mathbb{Z}$. (This is the same situation that we encountered when generalizing gcds and lcms.)

Except for this pedantic point, our notions of "irreducible" and "primes" do generalize prime numbers:

Proposition 1.14.14. Let $r \in \mathbb{Z}$. Then, we have the following equivalence:

$$(r \text{ is prime in } \mathbb{Z}) \iff (r \text{ is irreducible in } \mathbb{Z}) \iff (|r| \text{ is a prime number}).$$

Proof. Left to the reader. □

In particular, the prime elements of $\mathbb{Z}$ are not just the prime numbers $2, 3, 5, 7, 11, \ldots$ but also their negatives $-2, -3, -5, -7, -11, \ldots$. The irreducible elements of $\mathbb{Z}$ are the same.

Thus, in the ring $\mathbb{Z}$, being prime and being irreducible are the same thing. In an arbitrary integral domain, this is not always the case, as the following two examples show:

- In the ring $\mathbb{Z}\left[\sqrt{-5}\right]$, the element 3 is irreducible but not prime. (See [DumFoo04, §8.3] for the proof.)

- Here is an example using polynomials. Consider the univariate polynomial ring

  $$\mathbb{Q}[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ \mid \ a_0, a_1, \ldots, a_n \in \mathbb{Q} \right\}.$$

  This ring $\mathbb{Q}[x]$ has a subring

  $$\begin{aligned} R &= \left\{ a_0 + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \ \mid \ a_0, a_2, a_3, \ldots, a_n \in \mathbb{Q} \right\} \\ &= \left\{ \text{all polynomials } f \in \mathbb{Q}[x] \text{ whose } x^1\text{-coefficient is } 0 \right\} \\ &= \left\{ \text{all polynomials } f \in \mathbb{Q}[x] \text{ with } f'(0) = 0 \right\}. \end{aligned}$$

  Yes, this is a subring; check this!

> The element x^3 of R is irreducible (because if $x^3 = ab$ for two non-constant polynomials[2] a and b, then either a or b (or both) has a nonzero x^1-coefficient), but not prime (since $x^3 \mid x^2x^2$ but $x^3 \nmid x^2$ and $x^3 \nmid x^2$).

In each of these two examples, we found an element that is irreducible but not prime. Can the converse happen? No:

Proposition 1.14.15. Let R be an integral domain. Then, any prime element of R is irreducible.

Proof. Easy. (See Proposition 2.15.3 in the text.) □

In a PID, this goes both ways:

Proposition 1.14.16. Let R be a PID (for example, a Euclidean domain). Let $r \in R$. Then, r is prime if and only if r is irreducible.

Proof. Less easy, and I will say a few words about it next time. In a way, this proof is just an adaptation of the classical proof of Euclid's lemma from elementary number theory, which says that if a prime number p divides a product ab, then it divides a or b. □

References

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `https://site.uvm.edu/rfoote/files/2022/06/errata_3rd_edition.pdf` for errata.

[Knapp16] Anthony W. Knapp, *Basic Algebra*, Digital 2nd edition 2016.
`http://www.math.stonybrook.edu/~aknapp/download.html`

[Lehman19] James Larry Lehman, *Quadratic Number Theory*, Dolciani Mathematical Expositions **52**, MAA Press 2019.

[2] The units of the ring $\mathbb{Q}[x]$ are precisely the nonzero constant polynomials.